Valutazione della Sicurezza delle Reti Informatiche e Applicazione dei Sistemi SIEM

Relatori:
Chia.mo Prof. Michele SCALERA
Dott. Gennaro DEL CAMPO

Laureando:
Daniele PORCELLI

Dipartimento di Informatica - Università degli Studi di Bari
Via Orabona, 4 - 70125 - Bari
Tel: +39.080.5443270 | Fax: +39.080.5442536
serlab.di.uniba.it

Minacce dalla Rete

- La presenza di un'organizzazione in Internet la rende soggetta a minacce da parte di utenti malintenzionati (Hackers)
- Furto o compromissione dei dati, negazione di servizio

COSTI DELLE MINACCE

EURISPES
Dal 1982
l'Istituto di Ricerca
degli Italiani

- Gli attacchi informatici costano alle imprese **9 miliardi di euro** l'anno a causa di investimenti insufficienti, approcci di breve periodo e sottostime dei pericoli (rapporto Italia Eurispes 2017)

- Le PMI risultano essere in ritardo e quindi più soggette ad attacchi informatici (Clusit)

Clusit
Associazione Italiana
per la Sicurezza Informatica

COSTI DELLE MINACCE

- Gli attacchi informatici costano in media ad una PMI 175mila euro in 5 anni

- Nello stesso periodo di tempo, ne basterebbero dai 42mila ai 103mila euro per evitare che tali attacchi abbiano luogo

VALUTAZIONE DELLA SICUREZZA DELLE RETI INFORMATICHE

ATTACCHI INFORMATICI COME CONSEGUENZA

- Gli attacchi informatici sono una conseguenza di:
  - Configurazione poco attenta della rete informatica
  - Scarsa qualità del codice del software in esecuzione sulla rete da parte delle software house

PROCESSO DI VALUTAZIONE DELLA RETE

Attaccante

- Perlustrazione (Footprinting)
- Scansione dei servizi (Fingerprinting)
- Investigazione delle vulnerabilità
- Sfruttamento delle vulnerabilità

Difensore

- Investigazione delle vulnerabilità
- Sfruttamento delle vulnerabilità

APPROCCI PER LA VALUTAZIONE

- Automatica (Nessus, OpenVAS, Qualys, Rapid7 Nexpose)

- Manuale

- Una combinazione di entrambe per ottenere dei risultati più precisi e completi

Aree di valutazione

- Rete livello locale: VLAN, PNAC, STP, DHCP, PXE, WPAD…
- Rete livello IP: Rilevazione di sottoreti, host e servizi attivi; elusione di sistemi IDS/IPS
- Servizi di rete comuni: FTP, TFTP, SSH, Telnet, DNS, SNMP, LDAP, Kerberos…

I SISTEMI SIEM

Definizione di sistema SIEM

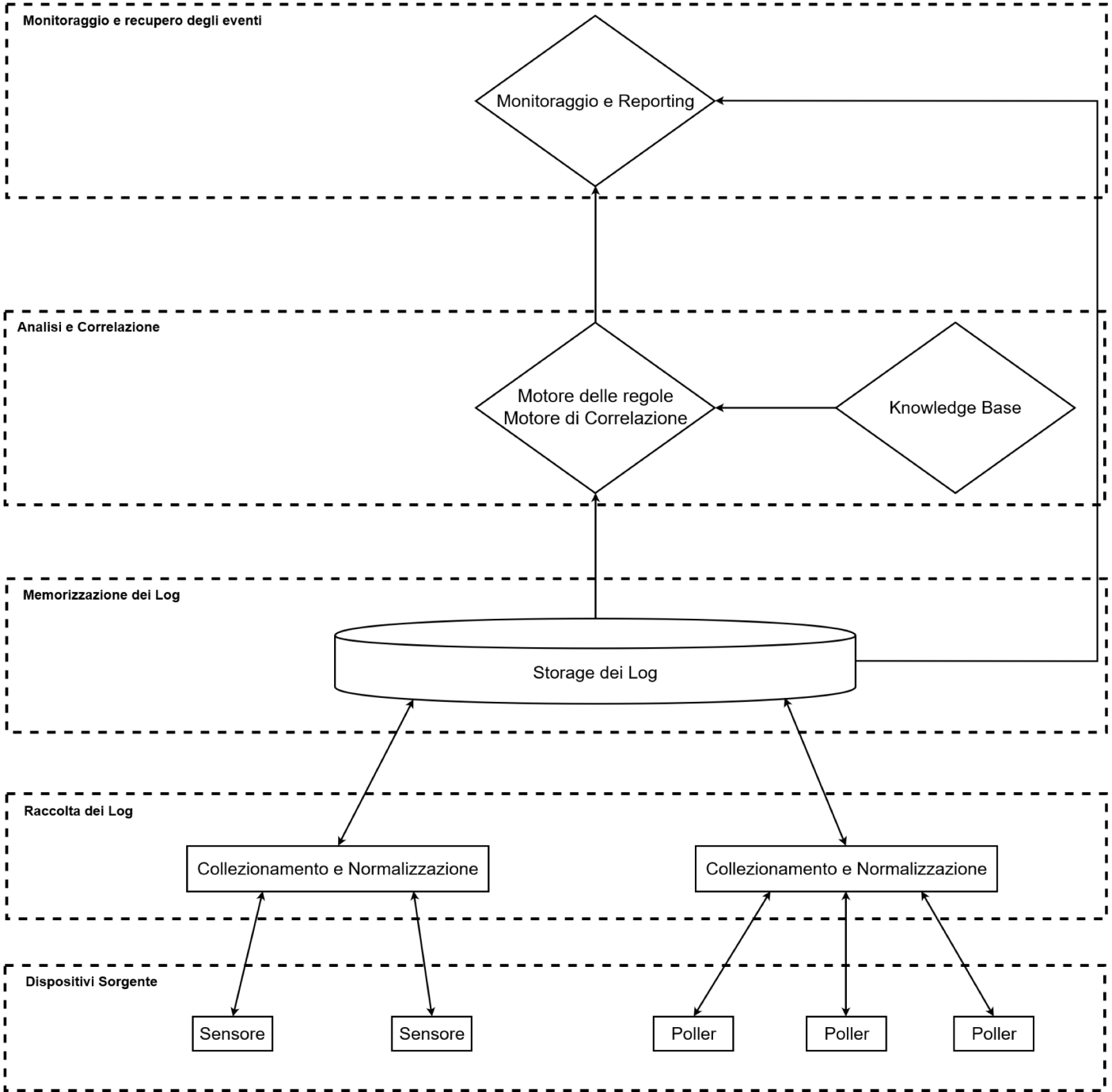
- Collezione di tecnologie che forniscono visione e chiarezza sul sistema informatico nel suo insieme
- Security Information Management (SIM): analisi e report di dati di log e memorizzazione a lungo termine
- Security Event Management (SEM): monitoraggio e notifiche in tempo reale
- SIM + SEM = SIEM: Security Information and Event Management

Funzioni di un sistema SIEM

- Log management: memorizzazione, organizzazione, recupero e archiviazione degli eventi (log) provenienti dai nodi della rete (router, switch, firewall, IDS, OS, applicativi)
- Conformità alle normative IT: consultazione degli eventi memorizzati per identificare violazioni ai requisiti di conformità che l'organizzazione deve rispettare (PCI DSS)

Funzioni di un sistema SIEM

- Correlazione degli eventi: correlazione di un evento con altri eventi per diminuire il numero di falsi-positivi
- Risposta attiva: reazione automatica ai potenziali attacchi rilevati
- Endpoint security: validazione e miglioramento dello stato di sicurezza degli host connessi alla rete


Monitoraggio e recupero degli eventi
Monitoraggio e Reporting
Analisi e Correlazione
Motore delle regole
Motore di Correlazione
Knowledge Base
Memorizzazione dei Log
Storage dei Log
Raccolta dei Log
Collezionamento e Normalizzazione
Collezionamento e Normalizzazione
Dispositivi Sorgente
Sensore
Sensore
Poller
Poller
Poller

ARCHITETTURA DI UN SIEM

- Dispositivi sorgente: switch, router, firewall, IDS, sistemi operativi, software applicativo




  - Sensori: generano eventi secondo una specifica operazione eseguita dai dispositivi sorgente (IDS)
  - Poller: generano eventi quando uno specifico stato viene rilevato su un sistema terzo (ping, openNMS)

ARCHITETTURA DI UN SIEM

- Raccolta dei Log: raccolta (pull) o ricezione (push) degli eventi generati dai dispositivi sorgente
  - Agent-based o Agentless
  - Filtraggio, normalizzazione e aggregazione degli eventi

ARCHITETTURA DI UN SIEM

- Memorizzazione dei Log:
  - Base di dati: scelta adottata dalla maggior parte dei sistemi SIEM
  - File di testo: facile lettura ma scarse prestazioni
  - File binario: buone prestazioni ma lettura impossibile da parte di esseri umani o altri programmi

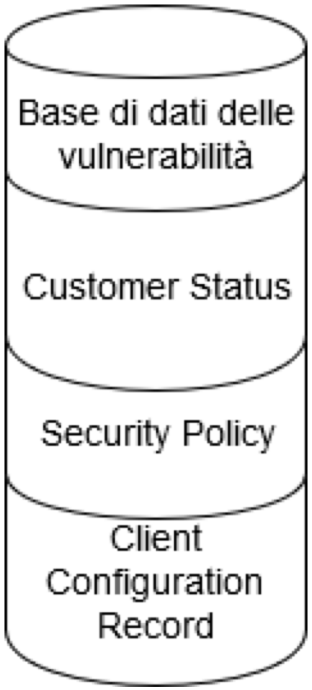
ARCHITETTURA DI UN SISTEMA SIEM

- Analisi e correlazione: gli eventi memorizzati vengono correlati tra di loro e vengono sottoposti alla verifica di alcune regole definite dall'utente per individuare potenziali attacchi

```
Se [(login falliti >= 3) e poi (Login Riuscito)] dalla stessa sorgente
          entro 20 secondi = Possibile Attacco Forza Bruta
```

ARCHITETTURA DI UN SISTEMA SIEM

- Knowledge Base: base di conoscenza di supporto al motore di analisi e correlazione per individuare e scartare falsi-positivi



ARCHITETTURA DI UN SISTEMA SIEM

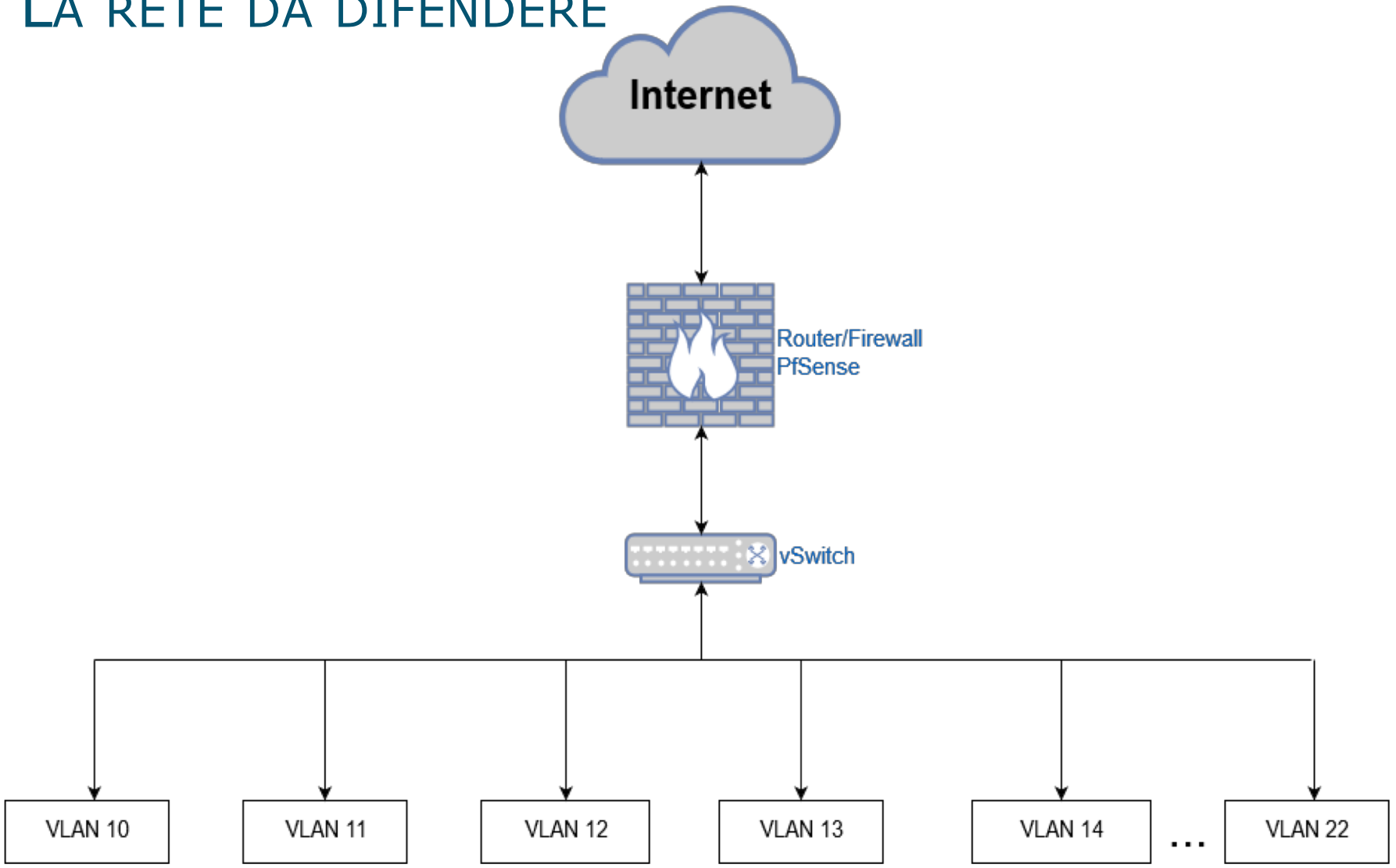
- Monitoraggio e recupero degli eventi: visualizza gli eventi memorizzati, dati statistici sulla sicurezza, report, stato di sicurezza dei sistemi, attacchi in corso, gestione dei ticket e delle procedure di risposta

SPERIMENTAZIONE

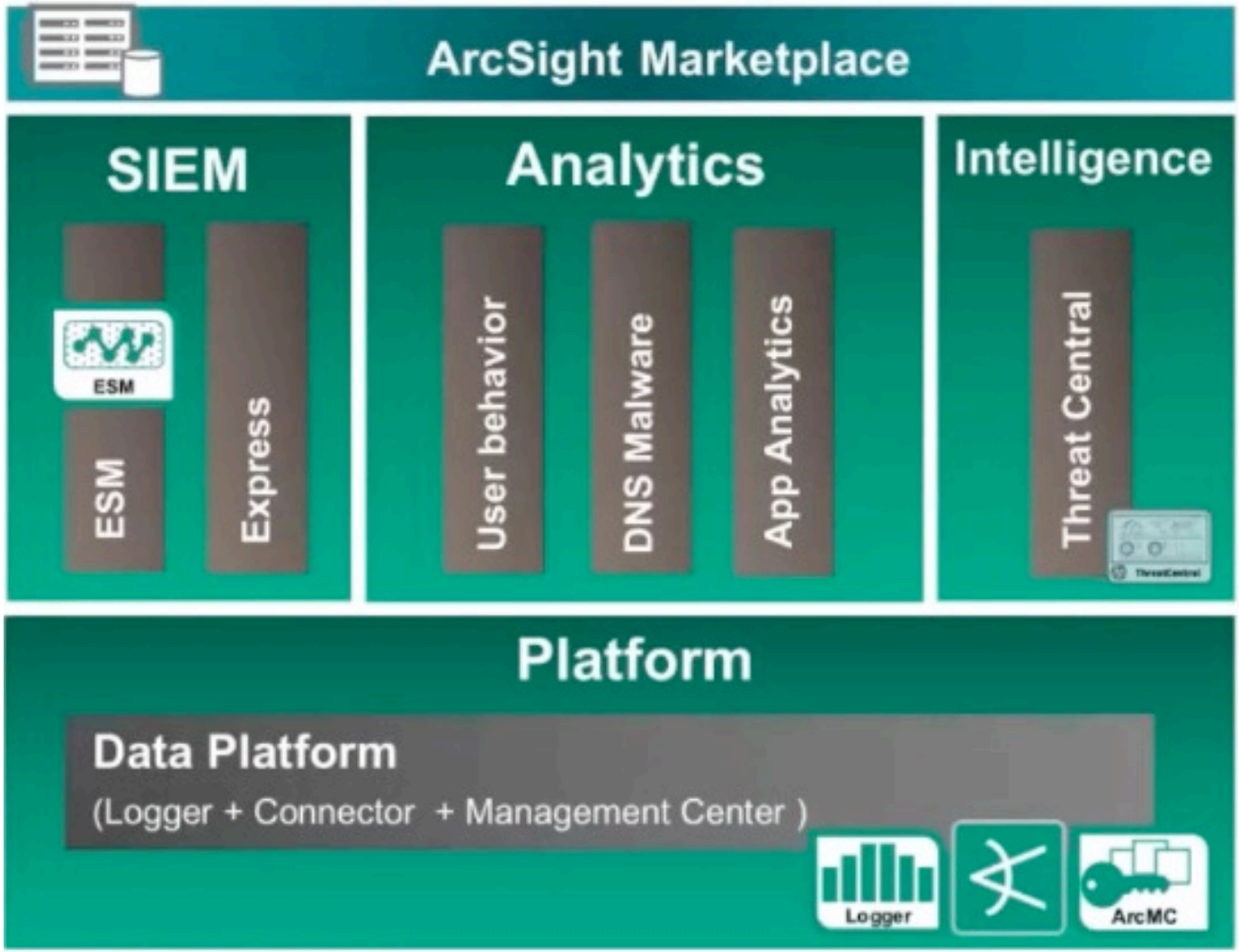
LA RETE DA DIFENDERE

- Virtual Data Center di SER&Practices utilizzato per lo sviluppo e test dei suoi progetti

LA RETE DA DIFENDERE



SOLUZIONE ADOTTATA: HPE ARCSIGHT



ARCSIGHT LOGGER

- Soluzione per le organizzazioni che necessitano di un'infrastruttura di log management:
  - Raccolta dei log
  - Archiviazione a medio e lungo termine
  - Funzioni di ricerca
  - Reporting
  - Aggregazioni dei log
  - Correlazioni semplici
  - Alerting e notifiche
  - Dashboard
  - Supporto all'analisi forense

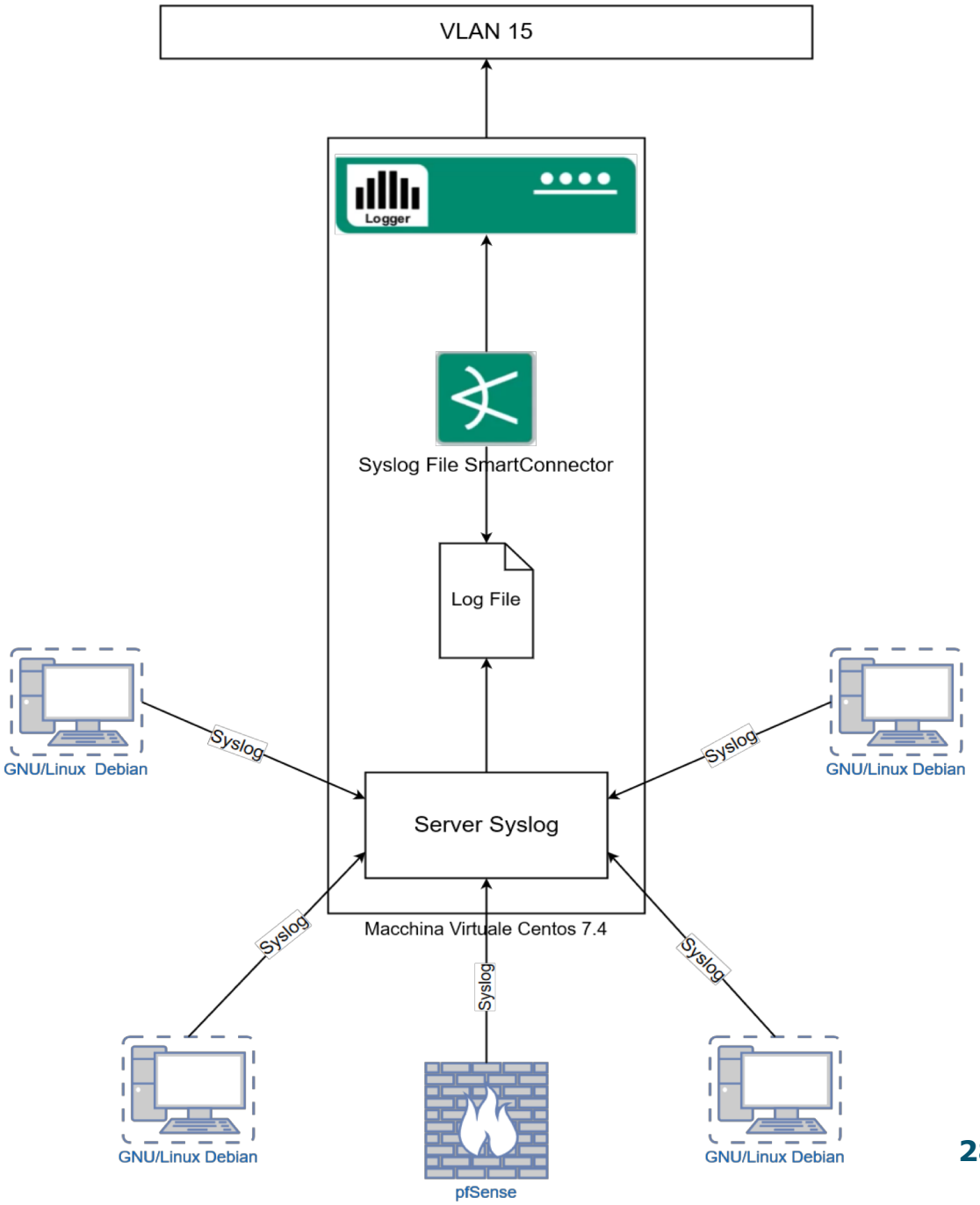
ARCSIGHT SMARTCONNECTOR

- Raccolgono gli eventi dai dispositivi sorgente
- Normalizzano i valori e il formato degli eventi (CEF)
- Filtrano gli eventi non necessari
- Aggregano gli eventi
- Categorizzano gli eventi raccolti
- Inviano gli eventi alla destinazione (Logger o ESM)

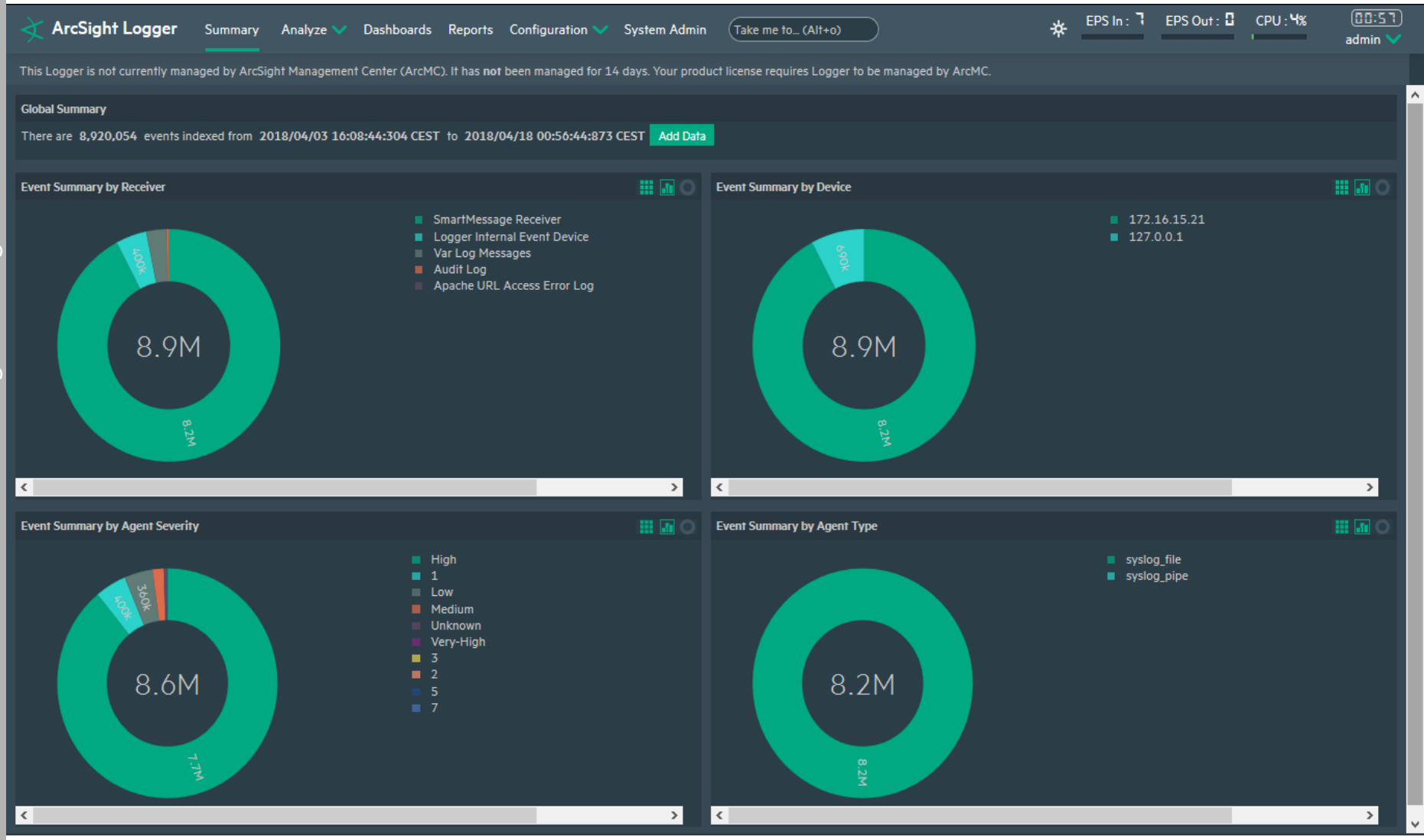
DEPLOYMENT

- Una macchina virtuale connessa alla VLAN 15 sulla quale è stato installato:
  - il sistema operativo GNU/Linux Centos 7.4
  - la soluzione Arcsight Logger
  - Un server Syslog (di default)
  - uno SmartConnector per gli eventi Syslog memorizzati in un file

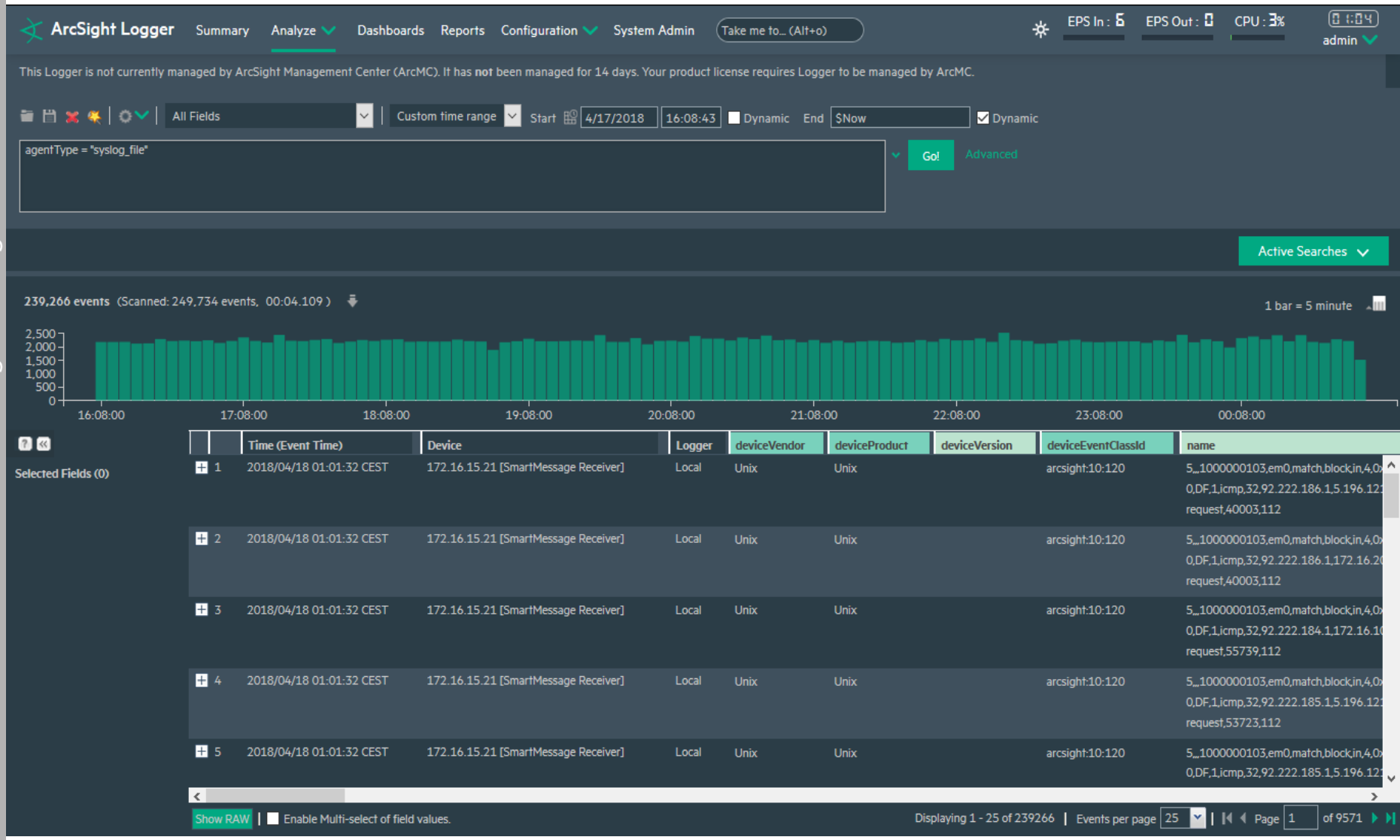
DEPLOYMENT


VLAN 15
Logger
Syslog File SmartConnector
Log File
Server Syslog
Macchina Virtuale Centos 7.4
GNU/Linux Debian
GNU/Linux Debian
GNU/Linux Debian
GNU/Linux Debian
pfSense
Syslog
Syslog
Syslog
Syslog
Syslog

ARCSIGHT LOGGER IN FUNZIONE



ARCSIGHT LOGGER IN FUNZIONE



Sviluppi futuri

- Integrazione di Arcsight ESM
- Deployment di un sistema IDS e di altri sistemi di sicurezza nel Virtual Data Center
- Integrazioni di altri SmartConnector (macchine Windows, Web server, DBMS, VPN…)
- Integrazione di Arcsight Management Center

GRAZIE PER L'ATTENZIONE